保安資訊--本周(台灣時間2022/12/30)
賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告(Protection Bulletins)。

關於 **保安資訊有限公司** ｜ 從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 83 萬 5,800 台受保護端點上總共阻止了1.077億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2022/12/26)**

- 在**15**萬**4,600**台端點上，阻止了**4,450**萬次嘗試掃描**Web**服務器的漏洞。
- 在**28**萬**3,800**台端點上，阻止了**2,310**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6**萬**300**台**Windows**伺服主機上，阻止了**1,680**萬次攻擊。
- 在**9**萬**8,300**端點上，阻止了**310**萬次嘗試掃描伺服器漏洞。
- 在**2**萬**3,900**台端點上，阻止了**130**萬次嘗試掃描在**CMS**漏洞。
- 在**5**萬**3,500**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**27**萬**5,200**台端點上，阻止了**660**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,500**台端點上，阻止了**250**萬次加密貨幣挖礦攻擊。
- 在**4**萬**5,800**台端點上，阻止了**510**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,200**台端點上，阻止了**14**萬**4,500**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

2022/12/30

基業長青～老牌Nanocore木馬，屹立不搖

Nanocore 是一種遠端存取木馬，即使在後起之秀異軍突起不斷的威脅領域中，它依舊屹立不搖， 仍然廣受不少駭客組織和個人所青睞。賽門鐵克持續觀察到使用這種惡意軟體的惡意行動。在過去的 25 天裡，我們看到許多電子郵件威脅攻擊行動散佈 Nanocore， 並鎖定世界各地各種規模的組織。這些攻擊型行動，採用的電子郵件主旨顯示，訂單、報價、轉帳和對帳單等常見的社交工程伎倆仍被廣泛採用。常見的例子如下：

- Amadeus ATC functionality
- APPLYING FOR THE POST OF AN ACCOUNTANT
- COMMERCIAL INVOICE AND BILL OF LANDING... 28/12/2022
- E-enquiry DAROU_ORDER_06122022
- E-enquiry JIAXING_ORDER_05122022
- ESSENTIAL OIL
- Letter of Recommendation
- New Order
- NEW ORDER 50708, 61062
- Orden de compra urgente 05-33062
- PAYMENT ACCOUNT STATEMENT / AGVE GROUP
- PAYMENT ACCOUNT STATEMENT / FENTEXmedical GmbH
- Request For Quote 100000pcs
- RETURN PAYMENT TT (Ref 001122022066743)
- Returned Payment
- Scan Copy_00206122022
- SUMMARY OF REMITTANCE TRF1038738
- Transfer Confirmation
- UPDATE EMAIL NOTIFICATION
- UPDATE EMAIL REQUIRED
- Urgent order=> KIND REMINDER (urgent)

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.PsDownloader!g1

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen285
- ISB.Downloader!gen544
- Trojan.Gen.MBT
- Scr.Malcode!gdn30
- Scr.Malcode!gdn34

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/29

氾濫的Chaos勒索軟體，針對意大利和土耳其組織

自原始碼被公開以來，賽門鐵克觀察到各種駭客組織和個人使用 Chaos 勒索軟體的多種變種。這些變種通常透過 RDP 暴力攻擊、軟體中的已知漏洞、偷渡式下載和惡意電子郵件等常見方法進行散佈。最近，已確定兩個特定的 Chaos 變種似乎以意大利和土耳其組織為目標，可能透過基於其名稱（faturra 和 sipari listesi）的惡意電子郵件。這些變種幕後的操控者並沒有採用雙重勒索戰術，也沒有將勒索軟體傳播到受害者基礎設施內的其他設備。這些變種的贖金要求相對較低，一個要求 500 美元，另一個要求 1600 美元，均以比特幣支付。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/28

注意PDF附件檔的危險性～IcedID銀行惡意軟體，利用惡意PDF附件檔，發動攻擊

IcedID 仍然是最熱門的銀行惡意軟體之一，僅次於 Qakbot。每天都會發生 IcedID 惡意垃圾郵件攻擊行動，這些行動幕後的操刀手透過不同的技術無休止地循環，意圖逃避安全機制的檢測。在最近的行動中，創作者一直夾帶惡意網路釣魚的 PDF 附件檔，如果成功被引誘，這些 PDF 會將受害者重定向到受密碼保護的壓縮檔。而該壓縮檔又包含另一個 ISO 檔的壓縮檔，其中包含一個會植入 IcedID 銀行惡意軟體的 LNK 捷徑檔案。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Trojan.Gen.MBT
- Trojan.IcedID

2022/12/27

PureLogs偷竊程式，透過惡意垃圾郵件行動散播

在當前的資安威脅態勢下，各式各樣的惡意軟體即服務，垂手可得。PureLogs 偷竊程式就是一種竊密程式，最近透過對其活動的仔細分析發現這樣一個例子。據報導，該惡意軟體正在意大利透過惡意電子郵件進行傳播。

PureLogs 偷竊程式的創作者被稱為“Pure Coder”。根據他們廣告，還提供其他類型的惡意軟體服務，包括加密程式、挖礦程式、惡意程式載入和遠端存取木馬。這些類型的惡意軟體即服務越來越普遍，對於個人和組織而言，重要的是要了解它們的各種傳播方式以及它們帶來的潛在風險。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.Mshta!g1
- SONAR.PsDownloader!g1
- SONAR.SuspScript!g5

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Suspicious: Content

基於機器學習的防禦技術：

- Heur.AdvML.B

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Activity - Bad Application Reputation Application 7
- System Infected: Trojan.Backdoor Activity 634

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/12/27

BlackHunt勒索軟體

最近有人發現到一個稱為“BlackHunt”的勒索軟體駭客集團，正在積極攻擊企業組織。該駭客集團也採用雙重勒索的戰術，威脅不就範支付贖金，就要公布他們手上竊得的機敏資訊。幾週前，受他們感染後出現藍底白字藍的當機電腦畫面會出現勒索說明。但是，最近他們一直在使用 HTA 和 TXT 格式的勒索說明。被該加密勒索軟體加密後的檔案，會被新增特定規則的副檔名，其中包括唯一的 ID、電子郵件聯絡人和“Black”字串。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/25

狼狽為奸～RisePro偷竊程式也開始與PrivateLoader合作

PrivateLoader 是一種按安裝次數付費的惡意軟體服務，協作攻擊發動者 (營運商) 向目標對象交付惡意有效籌載。它已被用於散佈各式各樣的惡意軟體，例如：GCleaner、Raccoon、Redline、Smokeloader 和 Vidar。最近有人觀察到它散佈一個名為 RisePro 的竊密程式，能夠從網路瀏覽器中竊取敏感資訊，例如：cookie、保存的密碼和信用卡資訊，以及加密貨幣錢包。PrivateLoader 通常透過搜索引擎優化 (SEO) 投毒進行傳播，誘使受害者下載並執行該惡意載入程式。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- SONAR.MalTraffic!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.MBT

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Bad Reputation Process Request 4
- System Infected: Trojan.Backdoor Activity 634
- Web Attack: Webpulse Bad Reputation Domain Request

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/12/23

Vidar竊密程式濫用各種社交媒體平台進行C&C通訊

Vidar 竊密程式繼續利用各種社交媒體平台進行 C&C 通訊。之前的行動已經觀察到惡意軟體與歸屬於威脅發動者的 Telegram 和 Mastodon 頻道進行通訊。不過最近，Vidar 變本加厲，濫用更多社交媒體平台，包括 Steam、TikTok 和 Ultimate Guitar。執行後，惡意軟體籌載會存取屬於威脅行為者的社交媒體頁面，並檢索配置檔案中發布的當前 C&C 伺服器 IP。這樣的設定允許攻擊者輕鬆且定期更改 C2 伺服器 IP 訊息，而無需對已經在真實網際網路上的惡意軟體樣本進行任何更改。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.Generic.616
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 704

2022/12/23

Bundlore廣告軟體，讓人有無寧日

Bundlore 是一種煩人的廣告軟體，多年來一直影響 Windows 和 MacOS 作業系統，並且不斷出現新版本。Bundlore 主要透過瀏覽網頁時的順道下載攻擊，偽裝成虛假的更新程式、破解程式和序號產生器程式來傳播，並且它沒有改變其策略。儘管存在已久，但它並沒有放緩的跡象，尤其是在 MacOS 上。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen

2022/12/22

防護亮點：賽門鐵克的郵件安全服務，成功瓦解Lokibot竊密程式的詭計

～防護亮點～

多年來，我們已多次發布有關 Lokibot 竊密程式的訊息--最近一次是在 12 月 14 日。至少可以追溯到 2015 年，Lokibot 透過永無止境的垃圾郵件攻擊行動進行傳播。這些壞蛋為數眾多且水平不一。Lokibot 通常利用附加在電子郵件中的惡意 PDF、RFT 和 Office 檔案作為感染媒介，並使用常見的報價、航運、銀行、SWIFT 外匯轉帳、發票和支付相關的社交工程主旨，Lokibot 試圖從包括瀏覽器在內的數百個應用程式中竊取憑證、FTP 用戶端、電子郵件用戶端、SSH 用戶端、加密貨幣錢包和密碼管理軟體。Lokibot 可能會使用幾種不同的打包工具來進行混淆，但最終必須在執行主要有效籌載之前將自己解壓縮到記憶體，終究還是會被發現。俗話說，國王根本沒有穿新衣。

賽門鐵克持續導入各種先進防護技術來預防及攔阻 Lokibot 的入侵意圖。縱深防禦 (多層次防護) 不僅僅是一個概念，它確實是保護您的組織的唯一方法。攻擊者整天不停歇地尋找您防禦機制中的弱點，即使是相對非頂尖的攻擊者--只要秉持純粹的僥倖或者莫名的好運--最終也會在您的一個或多個防護或流程機制中找到漏洞。但要找到一種能穿越多層防護的方法是一項更具挑戰性的任務。最好的防禦當然是主動防禦，在攻擊發生之前就已經牢固地進行保護。查看過去幾週我們的遙測監控系統清楚地表明多個 Lokibot 垃圾郵件攻擊行動，被賽門鐵克的多層次主動防禦技術所完全攔截，該防護技術集也成功攔截其他不同的威脅家族與種類。

賽門鐵克擁有領先業界的 **零時差** 保護技術，以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Packed.NSISPacker!g14

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

表列的檔案型檢測技術不僅適用於我們的電子郵件安全服務 (ESS)，還適用於所有採用我們檔案型檢測保護技術的賽門鐵克產品，包括 Symantec Endpoint Protection (SEP)、Data Center Security (DCS)、儲存保護、伺服器保護、網頁安全雲端服務和網頁安全閘道器 (SWG) 等。

要了解有關賽門鐵克雲端郵件安全服務的更多資訊，**請點擊此處下載我們型錄及簡報檔**。

2022/12/14

Lokibot在電子郵件領域的崛起

在這一點上，Lokibot 是大多數人都知道的竊密程式，它已經在資安威脅版圖嶄露頭角多年，現在流行率仍然很高。這種威脅已被用於竊取憑證和加密貨幣錢包，但也被用作部署第二階段惡意軟體的後門。最重要的是，它負責暗網上無數的憑證轉存(credential dumps)。

賽門鐵克持續每天觀察活動，但在過去幾週，我們發現惡意垃圾郵件活動有所增加。這些惡意垃圾郵件活動不使用時髦或花哨的社交工程手法，相反地，威脅發動者採用普通的報價、運輸、SWIFT、出貨明細及發票和支付相關的社交工程主旨。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.ProcHijack!g21

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.MBT

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Bad Reputation Process Request 4

基於機器學習的防禦技術：

- Heur.AdvML.B